ONC HEALTH IT CERTIFICATION PROGRAM

Program Policy Resource #18–03:

Surveillance Resource

(Last updated: October 5, 2018)

Table of Contents

I. INTRODUCTION 2

A. Background and Purpose 2

B. Companion Resources and Other Relevant Materials 2

C. Terminology 3

D. Text Boxes 4

II. SURVEILLANCE PLANS: CORE EXPECTATIONS AND SUBMISSION ELEMENTS 5

A. Preparation of Surveillance Plans 5

B. Submission Requirement and Deadline 5

III. APPROACH TO SURVEILLANCE 6

A. Reactive Surveillance 6

1. Duty to Initiate Reactive Surveillance 6

2. Weighing and Acting on Information About Potential Non-conformities 8

3. Employing Appropriate Surveillance Methodologies 9

B. Randomized Surveillance 10

IV. CONDUCTING SURVEILLANCE 10

A. Scope of Surveillance; Post-certification Conformity Assessments 11

B. Surveillance Methodology 13

1. Consistent Application of Surveillance Methodology and Approach 14

2. Working with Providers 16

C. Transparency and Disclosure Requirements: Surveillance of Developers' Disclosures 17

D. ONC Prioritized Capabilities and Requirements 18

V. CORRECTIVE ACTION 20

VI. SUBMISSION AND REPORTING OF SURVEILLANCE AND CORRECTIVE ACTION INFORMATION 22

A. Submission of Surveillance Information to ONC 22

1. Surveillance Narratives and Corroborating Documentation 22

2. Reporting Surveillance Information on CHPL 24

B. Due Process and Exclusion of Certain Sensitive Information 25

1. Meaningful Opportunity for Input and Comment on ONC-ACB Findings 25

2. Exclusion of Certain Information from Submission of Corrective Action Information and Surveillance Results 25

3. Exclusion of Certain Information from Submission of Corrective Action Information 25
C. Due Date and Submission Method for Surveillance Results 26
VII. DEVELOPER COMPLAINT PROCESSES 26
A. Review of Developer Complaint Processes 26
B. Reporting on Developer Complaint Processes 27
VIII. PUBLIC ACCOUNTABILITY 27

I. INTRODUCTION

A. Background and Purpose

Under the ONC Health IT Certification Program (**Program**), ONC-Authorized Certification Bodies (ONC-ACBs) are required to perform surveillance of the health information technology (health IT) they have certified (45 CFR 170.556 and 170.523(i)).[1] The Office of the National Coordinator for Health Information Technology (ONC) issues surveillance resources to clarify ONC-ACBs' responsibilities for conducting surveillance, to identify topics and specific elements of surveillance that ONC considers a priority, and to assist ONC-ACBs to develop their surveillance plans.

This Program Policy Resource #18-03 updates and replaces Program Policy Guidance #15-01A, issued November 5, 2015.

B. Companion Resources and Other Relevant Materials

This resource should be read and understood in conjunction with the following companion resources, which describe in detail many of the Program requirements referenced in this resource.

- Program Policy Resource #18–01: Post-certification Assessment of Program Requirements (**Post-certification Assessment Resource**).
- Program Policy Resource #18–02: Disclosure of Material Information (**Disclosure of Material Information Resource**).

ONC-ACBs should also review the following regulatory materials, which establish the core requirements and responsibilities for surveillance under the Program.

- 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications final rule, 80 FR 62601 (Oct 16, 2015) (**2015 Edition final rule**)
  - ↳ *Section IV.D.1 — "In-the-field" Surveillance and Maintenance of Certification*
  - ↳ *Section IV.D.2 — Transparency and Disclosure Requirements*

In addition, ONC-ACBs should be aware of the following final rules, which were promulgated after the issuance of Program Policy Resource #15-01A on November 5, 2015. These final rules contain additional requirements for certified health IT developers and for certain health care

[1] An ONC-ACB is deemed to "have certified" health IT if: (1) it has issued and has not withdrawn a certification to the health IT; or (2) it has assumed responsibility for a certification issued by another ONC-ACB and has not withdrawn the certification.

providers that enhance the surveillance, oversight, and accountability of health IT certified under the Program.

- On October 19, 2016, ONC published the ONC Health IT Certification Program: Enhanced Oversight and Accountability final rule, 81 FR 72404 (**EOA final rule**). The EOA final rule underscored the critical role of surveillance in protecting the effectiveness and integrity of the Program. The EOA final rule added additional requirements for ONC-ACBs in support of ONC's direct oversight of certified health IT products in certain situations and to further promote transparency and accountability under the Program.

- On November 4, 2016, the Centers for Medicare & Medicaid Services (CMS) published the Medicare Program: Merit-Based Incentive Payment System and Alternative Payment Model Incentive under the Physician Fee Schedule, and Criteria for Physician-Focused Payment Models final rule with comment period, 81 FR 77008 (**QPP final rule**). Relevant to this resource, the QPP final rule addresses the issue of health care provider cooperation with health IT oversight activities.

C. Terminology

To make this resource more accessible, plain language terms are used as a short-hand for certain regulatory concepts. The use of these terms is strictly for convenience and does not create any new requirements or alter the interpretation of existing requirements under the Program. When encountering any of the following terms noted in the table below in this resource, the reader should substitute the following definitions:

Table 1: Terminology Used in this Resource

Term	Definition
Compliance	With respect to a requirement of the Program, conformity with such requirement.
Developer	A person or entity that submits health IT for certification under the Program and/or is responsible for maintaining a certification issued to health IT under the Program.
in the field	With respect to certified health IT, as implemented and used in a production environment (as defined below).
non-conformity	The failure of certified health IT or of a certified health IT developer to conform to a requirement of the Program.
Product	A Complete EHR, Health IT Module, or other health IT that has been issued a certification or has been submitted for certification under the Program (as the context requires).
production environment	Any real-world setting (such as a hospital or doctor's office) in which the capabilities of certified health IT are implemented or used.
Program	The ONC Health IT Certification Program.
required capability or **certified capability**	A capability or other aspect of health IT that is required by one or more certification criteria to which the technology is certified, typically comprising one or more required outcomes (as defined below).
required outcome	Any characteristic that a product must possess or any outcome it must enable to support a required capability (as defined below).

Term	Definition
Technology	A "product" (as defined above).
Testing	The process of evaluating a product's performance under simulated and/or controlled conditions, including but not limited to testing conducted prior to certification under the supervision of an ONC-Authorized Testing Lab (ONC-ATL) in accordance with approved test procedures, testing tools, and, where applicable, test data.

D. Text Boxes

To assist ONC-ACBs to prepare their surveillance plans, a number of gray shaded text boxes appear throughout this document. The text boxes provide a roadmap and checklist for ONC-ACBs as they develop their surveillance plans. However, ONC-ACBs need to thoroughly review all parts of this resource and other materials cross-referenced herein and address all required aspects of surveillance in their surveillance plans.

II. SURVEILLANCE PLANS: CORE EXPECTATIONS AND SUBMISSION ELEMENTS

A. Preparation of Surveillance Plans

Each ONC-ACB must submit a surveillance plan (45 CFR 170.523(i)(1)) that describes—in detail and with requisite specificity—how the ONC-ACB will implement all required aspects of surveillance. The surveillance plans should address, at minimum, each topic area and issue identified in the shaded boxed sections of text below. ONC-ACBs are not limited to responding to the issues identified in those shaded text boxes. ONC-ACBs are encouraged to use the headings adopted in this resource to structure their surveillance plans.

In preparing their surveillance plans, ONC-ACBs should be mindful of their unique role and responsibility for ensuring the fundamental effectiveness and integrity of the Program. In keeping with the central importance of ONC-ACBs' surveillance activities to achieve core policies and objectives of the Program and recognizing that ONC-ACBs have accumulated a substantial body of experience through their surveillance activities to date, we expect surveillance plans to demonstrate a thorough understanding of the full range of requirements that apply to certified products and to developers under the Program. We also expect ONC-ACBs to provide detailed and comprehensive plans for consistently enforcing Program requirements, including a detailed description of relevant approaches and methodologies.

Surveillance plans should reflect ONC-ACBs' greater familiarity with the changes to certification criteria and other requirements of the Program that were adopted or clarified in the 2015 Edition final rule. In preparing their plans, ONC-ACBs are expected to evaluate their experiences, and any feedback from ONC, in relation to their surveillance activities in past years, including their surveillance of prioritized certification criteria and other prioritized requirements (such as the transparency and disclosure requirements at 45 CFR 170.523(k)).

Before preparing their surveillance plans, ONC-ACBs are expected to carefully review corresponding resources and related regulatory materials cited in Part I.B above, which provide important information and clarifications concerning many of the Program requirements and ONC-ACB surveillance responsibilities discussed in this document.

B. Submission Requirement and Deadline

Surveillance plans are due to ONC annually on **September 30th**. Extensions may be granted in limited circumstances and must be requested in writing with accompanying rationale no later than September15. ONC will only accept electronic submissions and requests for extensions, which must be submitted via ONC-ACB@hhs.gov.

III. APPROACH TO SURVEILLANCE

A. Reactive Surveillance

1. Duty to Initiate Reactive Surveillance

An ONC-ACB has a duty to perform ongoing reactive surveillance of certified health IT (45 CFR 170.556(b); 170.523(i)). The duty to initiate reactive surveillance is triggered whenever an ONC-ACB becomes aware of facts or circumstances (regardless of the source) that would cause a reasonable person to question whether a health IT product or a developer has complied with one or more requirements of the Program. When an ONC-ACB is aware of such information, it must initiate surveillance—including, as necessary, in-the-field surveillance in accordance with 45 CFR 170.556(a)—of the product or developer, as applicable.

While the duty to initiate surveillance applies for all Program requirements (80 FR 62712; see also 81 FR 72411), ONC-ACBs should pay particular attention to the requirements as interpreted and described in ONC's Post-certification Assessment Resource and Disclosure of Material Information Resource, which by their nature, can only be properly evaluated after a product has been certified and made available for use in production environments.

Overall Approach to Surveillance

Surveillance plans should describe clearly and in significant detail the ONC-ACB's overall approach to conducting reactive surveillance of certificates and developers. The plan should demonstrate the ONC-ACB's thorough understanding of its surveillance responsibilities and of the full range of requirements under the Program, including by comprehensively addressing all required elements and other considerations described in this document and detailing sound approaches and methodologies for performing all applicable aspects of surveillance under the Program.

To execute on their reactive surveillance responsibilities, ONC-ACBs need to actively monitor and seek out information about the performance of certified health IT products and capabilities as well as information about the manner in which developers market and make such products and capabilities available to customers and users.

As a starting point, ONC-ACBs are required to have in place processes for users and any other interested persons to submit complaints or other information about certified health IT products or developers directly to an ONC-ACB. ONC-ACBs should be prepared to receive and appropriately handle such information, including by responding to complaints and other information that they receive with appropriate urgency.

Process for Receiving Complaints and Other Information

Surveillance plans should describe the ONC-ACB's processes for allowing users and other stakeholders to submit information about certified health IT products and developers to the ONC-ACB.

In addition to responding to complaints and information that are submitted directly to them, ONC-ACBs should proactively identify other sources of information that will allow them to detect potential problems or issues that may trigger their duty to initiate reactive surveillance.

Consistent with prior years' practice, we expect ONC-ACBs to automatically initiate surveillance of a Complete EHR or Health IT Module upon the issuance of 3 or more inherited certified status requests.[2]

Obtaining, Synthesizing, and Acting on Information on Product Performance

Surveillance plans should detail how the ONC-ACB will systematically obtain, synthesize, and act on information concerning ongoing compliance with certification requirements, including but not limited to the following information:[3]

- Developers' complaint logs and defect tickets (including documentation concerning the developer's root cause analysis and information about the resolution of tickets) (see Part VII below).
- Developers' public and private disclosures with customers and prospective customers regarding certified health IT capabilities. Surveillance plans should also describe how that information is used to inform the ONC-ACB's decision to initiate surveillance of a developer's compliance with the disclosure requirements at 45 CFR 170.523(k)(1) and, separately, to identify instances in which the failure to disclose limitations or additional types of costs associated with certified capabilities could substantially impair their use.
- Information from publicly available sources (e.g., trade media, a developer's website, or user forums) regarding the ongoing compliance of certified products and developers with Program requirements. The ONC-ACB's plan should identify, at minimum, examples of the sources that the ONC-ACB will review, and the frequency of that review.
- Repeated inherited certified status requests and other "automatic triggers" for ONC-ACB reactive surveillance.
- If the ONC-ACB proposes to use survey instruments to obtain information:
  - ↳ The survey method(s) to be used by the ONC-ACB;
  - ↳ The subjects (e.g., health IT users, health information exchanges, third party integrators etc.) that the ONC-ACB will survey;
  - ↳ The ONC-ACB's survey program; and
  - ↳ The ONC-ACB's approach to interpreting survey results and determining when to initiate reactive surveillance in response to survey results.
- Complaints and other information about certified health IT submitted directly to the ONC-ACB by customers or users of certified health IT, by ONC,[4] or by other stakeholders. ONC-ACB surveillance plans should describe how the ONC-ACB will distinguish between complaints or information that do and do not raise issues within the scope of certification and an ONC-ACB's surveillance responsibilities.
- The ONC-ACB's experience with a particular certified product.

[2] *See* ONC Health IT Certification Program Guidance, #13-01, #14-01, and #15-01A, https://www.healthit.gov/policy-researchers-implementers/onc-health-it-certification-program-guidance.

[3] ONC-ACBs must require, as an ongoing condition of certification, that health IT developers furnish to the ONC-ACB upon its request all information the ONC-ACB determines necessary to carry out its surveillance responsibilities. A refusal by a health IT developer to provide all necessary information to an ONC-ACB may be regarded by an ONC-ACB as a refusal to participate in surveillance under the ONC Health IT Certification Program and the ONC-ACB shall institute appropriate procedures, consistent with the ONC-ACB's accreditation to ISO 17065, to withdraw any associated health IT Module/Complete EHR certification. 80 FR 62716.

[4] When ONC receives a user complaint about health IT, ONC's general practice is to forward the complaint to the ONC-ACB responsible for performing surveillance for that product under the ONC Health IT Certification Program. This general practice will not change as a result of the EOA final rule.

- Other facts and circumstances about which the ONC-ACB is aware.

2. Weighing and Acting on Information About Potential Non-conformities

In determining whether to initiate reactive surveillance, an ONC-ACB must consider and weigh the volume, substance, and credibility of complaints and other information received against the type and extent of the alleged non-conformity, in light of the ONC-ACB's expertise and experience with the particular capabilities, health IT, and certification requirements at issue (80 FR 62713).[5]

The following table illustrates some (though not all) factors that may be relevant to an ONC-ACB's determination whether to initiate surveillance on the basis of information about potential non-conformities. It is important to note that no single factor is dispositive and that different factors may point in different directions in a given case. For example, while the fact that an ONC-ACB has received only a single complaint may, standing alone, weigh against initiating surveillance, other factors such as the seriousness and credibility of the complaint may weigh in favor of initiating surveillance. ONC-ACBs should balance these factors and any other relevant information in order to determine whether a reasonable person would question the continued conformity of the certified product at issue.

Factors that may weigh *in favor* of initiating surveillance	**Factors that may weigh *against* initiating surveillance**
Volume	
Multiple complaints or sources of information	Isolated complaint or source of information
Credibility	
Complaint or information is detailed and specific	Complaint or information lacks detail or specificity
Source of complaint or information appears credible, such as where the source has first-hand knowledge or has previously proved reliable	Source of complaint may be unreliable, such as where the complainant is anonymous or has made previously disproven allegations

[5] The 2015 Edition final rule provides the following illustration of how these principles may be applied in practice (80 FR 62713):

> [I]f an ONC-ACB receives a number of anonymous complaints alleging general dissatisfaction with a particular certified Health IT Module, the ONC-ACB is not required to initiate surveillance (though it would not be precluded from doing so). In contrast, if an ONC-ACB receives several complaints alleging, for example, that a particular certified Health IT Module is unable to electronically create a set of export summaries in accordance with [45 CFR 170.315(b)(6)], the ONC-ACB should initiate surveillance of the Health IT Module unless a reasonable person in the ONC-ACB's position would doubt the credibility or accuracy of the complaints. A reasonable basis for doubt might exist if the ONC-ACB had recently responded to the very same issue and determined through in-the-field surveillance of the Health IT Module at several different locations that the reported problem was due to a "bug" arising from an unsupported use of the Health IT Module that the developer had specifically cautioned users about in advance.

Factors that may weigh *in favor* of initiating surveillance	Factors that may weigh *against* initiating surveillance
Substance	
Violation of Program requirements seems plausible, at least on the face of the information and based on the ONC-ACB's expertise and experience with the particular capabilities, health IT, and certification requirements at issue	Violation of Program requirements seems implausible in light of the ONC-ACB's prior surveillance and other expertise and experience with the particular capabilities, health IT, and certification requirements at issue
Complaint or information alleges a serious problem, e.g., a risk to public health or safety or problems that could impact a large number of users.	
Complaint or information concerns a prioritized capability, the failure to disclose material information, or a limitation or additional type of cost that may interfere with a user or potential user's ability to implement or use certified capabilities for any purpose reasonably within the scope of the technology's certification.	

An ONC-ACB's decision to initiate reactive surveillance must also take into account complaints and other information indicating whether a developer has disclosed all known material information about certified capabilities required by 45 CFR 170.523(k)(1) (80 FR 62713). Importantly, ONC-ACBs should consider not only the likelihood of a disclosure violation but also the potential impact of the potentially undisclosed limitation or additional type of cost on potential users of the certified health IT. For example, where a developer fails to disclose a material limitation or additional type of cost and, as a result, customers or users experience unanticipated implementation or other challenges that substantially interfere with their ability to successfully implement or use a required capability or to realize a required outcome, the interference with the product's certified capabilities is a non-conformity to the applicable certification criteria (80 FR 62711–13). In these circumstances, the ONC-ACB must require the developer to take corrective action not only to cure the defective disclosure but to restore the full use of the required capabilities for customers and users who have been or may become affected. ONC-ACBs should refer to the Post-certification Assessment Resource and the Disclosure of Material Information Resource for additional information on this and related issues.[6]

3. Employing Appropriate Surveillance Methodologies

Whether reactive surveillance must include in-the-field surveillance or may employ other methods is governed by the definition and principles for in-the-field surveillance described in the 2015 Edition final rule (*see* 80 FR 62712) and codified at 45 CFR 170.556(a). Relevant con-

[6] For further discussion of impermissible interferences with the implementation or use of certified capabilities—including impermissible limitations and additional types of costs—refer to the Post-certification Assessment Resource, Part III.E.2, and the provisions of the 2015 Edition cited therein. For information about corrective actions that a developer may need to take to correct a disclosure violation and/or an impermissible limitation or additional type of cost, see Part IV of the Disclosure of Material Information Resource.

siderations include the nature of the suspected non-conformity and the adequacy of other forms of surveillance under the circumstances. These and other matters to be considered when determining the appropriate method and manner of surveillance are discussed in the 2015 Edition final rule (*see* 80 FR 62713) and in Part IV below.

Approach to Employing Surveillance Methodologies

Surveillance plans should describe how the ONC-ACB will determine for each instance of surveillance the appropriate conformity assessment techniques and methodologies to employ, including the factors that the ONC-ACB will use in determining whether to conduct surveillance of the technology in the field.

We note that ONC-ACBs must always review developers' disclosures whenever they perform reactive surveillance. 45 CFR 170.556(b)(1). ONC-ACBs should refer to ONC's Disclosure of Material Information Resource for detailed information about the requirements to be met by developers in order that they comply with 45 CFR 170.523(k)(1).[7]

ONC-ACBs should also explain how they will weigh and act on information about other aspects of surveillance prioritized by the National Coordinator in Part IV.D below.

B. Randomized Surveillance

ONC has exercised enforcement discretion with respect to the implementation of randomized surveillance by ONC-ACBs.[8] Regulatory requirements at 45 CFR 170.556(c)(2) dictate that ONC-ACBs conduct randomized in-the-field surveillance for, at a minimum, two percent of the health IT certifications they have issued. As of September 21, 2017, ONC will not, until further notice, audit ONC-ACBs for compliance with randomized surveillance requirements or otherwise take administrative or other action to enforce such requirements against ONC-ACBs, nor will it consider lack of implementation of these requirements by an ONC-ACB to be a violation of its compliance requirements under 45 CFR 170.566, the Principles of Proper Conduct for ONC-ACBs, or good standing under the ONC Health IT Certification Program (Program).[9]

IV. CONDUCTING SURVEILLANCE

Consistent with ONC-ACBs' responsibilities under the Program, ONC-ACBs must perform surveillance of certified health IT "in the field" as necessary to determine whether the technology continues to conform to the requirements of its certification once implemented and in use in a production environment. In-the-field surveillance is a key part of an ONC-ACB's approach to surveillance. 45 CFR 170.556(a)–(c).

[7] An ONC-ACB's decision to initiate reactive surveillance must take into account complaints and other information indicating whether a health IT developer has disclosed all known material information about certified capabilities, as required by 45 CFR 170.523(k)(1) (80 FR 62713). The failure to disclose this information calls into question the continued conformity of those capabilities because it creates a substantial risk that existing and prospective users will encounter problems implementing the capabilities in a manner consistent with the applicable certification criteria (*Id.*). Where an apparent failure to disclose known material information raises these potential concerns regarding the performance of certified health IT capabilities, an ONC-ACB would be required to initiate in-the-field surveillance to determine both whether the developer had failed to disclose the information and, if so, whether the failure to disclose the information prevented users from reasonably implementing and using certified capabilities for any purpose within the scope of the health IT's certification (*Id.*).

[8] *See* https://www.healthit.gov/sites/default/files/ONC_Enforcement_Discretion_Randomized_Surveillance_8-30-17.pdf

[9] ONC-ACBs should continue good faith execution of any active and ongoing randomized surveillance to ensure product compliance with the Program. If an ONC-ACB chooses to conduct randomized surveillance, the ONC-ACB should follow the methodology for randomized surveillance identified by ONC with respect to scope (45 CFR 170.556(c)(1)), selection method (45 CFR 170.556(c)(3)), and the number and types of locations for in-the-field surveillance (45 CFR 170.556(c)(4)).

Overall Approach to Conducting Surveillance

Surveillance plans should describe:

- an ONC-ACB's overall approach to conducting surveillance of certified products,[10] including specific methodologies it intends to use when surveilling products and developers and assessing their compliance with Program requirements; and
- an ONC-ACB's approach to thoroughly documenting its surveillance activities and keeping accurate and complete records that facilitate an ONC-ACB's reporting requirements as specified in Part VI.A below.

A. Scope of Surveillance; Post-certification Conformity Assessments

An ONC-ACB's surveillance of certified health IT is not limited to aspects of the technology that were tested in a controlled environment. While testing is an important part of an ONC-ACB's overall analysis of health IT under the Program, it focuses on particular use cases and necessarily reflects assumptions about how capabilities will be implemented and used in practice. Thus, while test results provide the initial indication that health IT meets the requirements of its certification and can support the capabilities required by the certification criteria to which the technology was certified, that determination is subject to an ONC-ACB's ongoing surveillance, including the ONC-ACB's evaluation of certified capabilities in the field.

The 2015 Edition final rule discusses several circumstances under which health IT would no longer conform to the requirements of its certification, including several examples of non-conformities in the field that would not occur during testing in a controlled environment.[11] Additional examples are available in the Post-certification Assessment Resource, which provides detailed on the assessment of certification requirements after health IT has been certified.

Because testing focuses on discrete and narrowly-defined outcomes that can be readily demonstrated in a testing laboratory, many required capabilities and outcomes that need to be supported or demonstrated by a certified product are assessed for the first time when an ONC-ACB performs surveillance of certified products. Some important examples of Program requirements that are assessed in the "post-certification" surveillance phase include:

- **Performance of certified capabilities when they are implemented and used in the field**. Certified products must support the full range of intended capabilities, uses, and other outcomes covered by applicable certification criteria, not just the specific functionalities, workflows, and other aspects that were demonstrated at the time the product was tested and certified (80 FR 62711; 81 FR 72412). Relatedly, developers must make certified capabilities available in such a manner that they can be implemented and used in production environments for their intended purposes (80 FR 62710). Conversely, developers are prohibited from taking any action that is likely to limit, restrict, or otherwise substantially interfere with the use of certified capabilities for such purposes (80 FR 62711).
- **Disclosure of known material information about certified products.** Pursuant to 45 CFR 170.523(k)(1), developers must publicly disclose detailed, plain-language information about

[10] We clarify that by "conducting surveillance" we mean assessing whether a product or developer selected for surveillance complies with Program requirements, including requirements that were demonstrated prior to certification as well as requirements of the Program that must be evaluated *after* a product is marketed to customers or deployed in production environments.

[11] For example, an ONC-ACB would find a non-conformity were it to determine that a developer had imposed restrictions or limitations on its technology (or the use of its technology) that substantially interfered with users' ability to access or use certified capabilities for any purpose within the scope of the technology's certification. Additional examples and discussion of such non-conformities are provided in the 2015 Edition final rule at 80 FR 62709–11.

known material limitations and additional types of costs that a customer or user may encounter to successfully implement or use certified capabilities (80 FR 62722).

- **Other developer responsibilities that ensure the overall integrity and effectiveness of the Program.** These requirements include submitting certain information related to developer's certified products and cooperating with processes for the testing, certification, and surveillance of health IT under the Program.

ONC's Post-certification Assessment Resource provides specific information about the post-certification assessment of these Program requirements. As explained in that resource, the post-certification assessment of Program requirements is not an exercise in "re-testing" the ability of products to pass the ONC approved test procedures or to demonstrate expected outcomes in a testing lab or other controlled environment. Rather, in a post-certification assessment of Program requirements the ONC-ACB should exercise of substantial professional judgment and consider the full intended scope of certification criteria and other requirements, in light of the unique context in which certified products and capabilities are marketed and made available for use in production environments.

Performing Post-certification Assessments of Conformity

Surveillance plans should thoroughly describe how the ONC-ACB will assess the performance of health IT products once they have been certified, including but not limited to the requirements noted above and in ONC's Post-certification Assessment Resource. Among other factors, plans should specifically describe how the ONC-ACB will:

- Assess compliance with Program requirements in the field, taking into consideration the unique circumstances and context in which certified health IT is marketed, implemented, and used.
- Identify capabilities and uses that are within the scope of applicable certification criteria but were not tested (or cannot be tested) in a controlled environment.
- Assess whether certified products are able to support such required capabilities and uses in production environments.
- Assess whether developers have substantially interfered with the use of such required capabilities or uses in any way, including through the imposition of material limitations or additional types of costs.
- Evaluate the performance of certified capabilities, including whether such capabilities consistently perform in an accurate and reliable manner when deployed in production environments, to the extent that such factors are reasonably within the control of the developer.
- Surveil developers' websites, marketing materials, and other communications to ensure strict adherence to the disclosure requirements at 45 CFR 170.523(k)(1), including the detailed and prominent disclosure of plain-language information about known material limitations and additional types of costs.
- Periodically review developers' publicly accessible online disclosure statements to ensure that they are correctly linked to the CHPL and provide a comprehensive and up-to-date list of all mandatory disclosures for all of the developer's certified health IT products.
- Ensure that developers adhere to other requirements that are necessary to the basic integrity and effectiveness of the Program, including the requirement for developers to cooperate with processes for the surveillance of health IT and to not take any action that could undermine or circumvent those processes.

B. Surveillance Methodology

Whether an ONC-ACB must perform in-the-field surveillance or may employ other methods is governed by the definition and principles for in-the-field surveillance codified at 45 CFR 170.556(a), as elaborated in the preamble to the 2015 Edition final rule (80 FR 62708–09). Among other factors, an ONC-ACB should consider the nature of the suspected non-conformity and the adequacy of other forms of surveillance for evaluating the suspected non-conformity under the circumstances.[12]

In-the-field surveillance may also be necessary to determine a developer's compliance with certification program requirements, such as the disclosure requirements at 45 CFR 170.523(k)(1). While non-compliance with the requirements of 45 CFR 170.523(k)(1) may often be established from complaints and a review of a developer's disclosures, certain kinds of undisclosed limitations or additional types of costs associated with certified capabilities may need to be confirmed through in-the-field surveillance of the technology, or may not be discovered at all except upon observing the operation of certified capabilities in the field. Indeed, an ONC-ACB will typically need to conduct in-the-field surveillance to determine whether any limitation or additional type of cost identified by the ONC-ACB (or brought to its attention in a complaint or other information) is likely to substantially interfere with a customer or user's ability to access or use a certified capability for a purpose within the scope of the technology's certification.

Surveillance Methodology

Surveillance plans should explain how ONC-ACBs will evaluate factors arising from the unique circumstances and contexts in which certified health IT is implemented and used in the field, including:

- What criteria and methodologies the ONC-ACB will apply in determining whether and under what circumstances to initiate in-the-field surveillance of certified health IT.
- How the ONC-ACB will decide which capabilities and/or Program requirements to evaluate in the field.
- What methodologies and techniques the ONC-ACB will employ when actually observing and evaluating the use of certified capabilities and developers' compliance with Program requirements in the field.
- What other investigative and diagnostic techniques the ONC-ACB will use to supplement its in-the-field observations (e.g., user feedback, reviewing developers' complaint logs and resolution of complaints, replicating reported problems in a controlled environment, and other appropriate techniques).
- How the ONC-ACB will engage and work with developers and end-users to analyze and determine the causes of issues.
- How the ONC-ACB will evaluate potential non-conformities resulting from implementation or business practices of the developer that could affect the performance of certified capabilities in the field.[13]

[12] In most cases, the need to evaluate the certified health IT in the field will be obvious from the nature of the suspected non-conformity. For example, if a problem with a certified health IT capability is reported to arise only in connection with a specific local implementation option, an ONC-ACB would likely need to observe the relevant capabilities in the field in order to fully analyze the cause of the problem and determine whether it is the result of a non-conformity. In other cases, the need for in-the-field surveillance may become apparent only after other surveillance methods and techniques have failed to isolate the cause of the problem (80 FR 62708–09).

[13] *See supra* note 11 and accompanying text.

- How the ONC-ACB will evaluate potential non-conformities resulting from the non-disclosure of material information about limitations or additional types of costs associated with certified health IT.[14]
- How the ONC-ACB will document its findings, analysis, and conclusions.

1. Consistent Application of Surveillance Methodology and Approach

An ONC-ACB should consider the circumstances and context in which the certified health IT is implemented and used in order to properly assess whether it continues to perform in the field in a manner that complies with its certification. Furthermore, individual health care providers are likely to have different preferences as to how surveillance is carried out, and should have the flexibility to work with ONC-ACBs to identify an approach to surveillance activities in the implementation setting that is most effective and convenient for them.

a. On-premises vs. Remote Observation

Surveillance activities may be performed through an in-person site visit to a provider's location or by remote observation. ONC-ACBs should take into account a provider's preference for a particular form of observation when determining how it will observe the health IT as part of surveillance activities. However, ONC-ACBs should also recognize that certain health IT performance issues can only be observed in a practice setting. In reaching a determination that in-the-field surveillance can be carried out by remote observation, ONC-ACBs should satisfy themselves that:

- they will be observing the use of the surveilled capability in the live production environment in which the capability has been implemented, or a test system that precisely mirrors the production environment;
- remote observation will not impact the ONC-ACB's ability to observe how the surveilled capability is integrated with other systems, processes, and workflows; and
- remote observation will be adequate to assess the nature, extent and full impact of any putative limitations, costs or actions by the developer that may be interfering with a user's ability to access or use a certified capability for a purpose within the scope of the product's certification.

If an ONC-ACB is unable to satisfy itself of these matters, it should not accede to a provider's stated preference for remote observation. Likewise, ONC-ACBs should not be guided by developer preferences for a particular observation method and should form an independent determination as to which observation is most appropriate in each instance.

Surveillance plans should describe how ONC-ACBs will determine the most appropriate method for observing the performance of certified health IT as part of surveillance. This shall include identifying the factors that the ONC-ACB will consider and weigh when making its determination.

[14] *See infra* Part IV.C hereof. The failure to disclose known material information about certified health IT is a violation of an explicit Program requirement (45 CFR 170.523(k)(1)) and thus constitutes a non-conformity. 80 FR 62601, 62711. In addition, the disclosure violation may also give rise to a separate non-conformity in the event that the failure to disclose the required information has substantially impaired, or would be likely to substantially impair, the ability of one or more users (or prospective users) to implement or use the developer's certified health IT in a manner consistent with its certification. *Id.*

b. Using in the field / production data

An ONC-ACB's assessment of a certified capability must be based on the use of the capability in the live production environment in which the capability has been implemented and is in use (45 CFR 170.556(a)(1)) and must use production data unless test data is specifically approved by the National Coordinator (45 CFR 170.556(a)(2)). The use of test data may be allowed in some circumstances, but may not be appropriate in all circumstances. For example, a problem with certified EHR technology capabilities may be difficult or impossible to replicate with test data. More fundamentally, limiting in-the-field surveillance to observations of test data would not provide the same degree of assurance that the certified EHR technology used by health care providers (i.e., production systems used with production data) continues to meet applicable certification requirements.

Using Test Data

Surveillance plans should state whether and under what circumstances the ONC-ACB proposes to use test data as part of in-the-field surveillance of certified health IT. The ONC-ACB's surveillance plan should also describe the assurances that the ONC-ACB will provide to ONC about the appropriateness of the proposed use of any test data. At a minimum, the ONC-ACB should determine whether the use of test data would yield similar product behavior and be equally comprehensive to data used in production systems.

c. Use of ONC Approved Test Procedures/Tools/Surveillance Data

To evaluate functionality and provide an initial indication of conformity, ONC-Authorized Testing Laboratories (ONC-ATLs) must use and ONC-ACBs may only certify health IT that has been tested using ONC Approved test procedures and test tools/data (45 CFR 170.523(h)). This initial testing permits evaluation of the performance of health IT in a controlled setting, under simplified scenarios and assumptions that can be readily demonstrated in an ONC-ATL testing environment. As discussed in the Post-certification Assessment Resource, these test methods prior to certification (including test procedures), along with any surveillance that follows certification, can together form the basis for assessing the full scope of certified capabilities and associated outcomes that certified health IT must be able to support in the field.[15] Thus, while ONC-ACBs may refer to historical ONC-ATL test results which informed their initial certification decision as a starting point for their in-the-field assessments, they should not rely exclusively on test results or ONC-approved test methods and should utilize other methodologies and approaches to obtain adequate assurances that certified products conform to the full range of relevant requirements.

In The Field Surveillance Assessment/Testing Approach

Surveillance plans should describe how ONC-ACBs will use ONC-ATL test results and ONC Approved test methods, if at all, as part of the conduct of the ONC-ACB's in the field surveillance activities. Additionally, the plans will address the ONC-ACBs approach to in the field surveillance assessment of conformity using production data and the implementation setting's workflow.

[15] *See* Post-certification Assessment Resource, Part II.B.

d. Developer participation in surveillance activities

ONC-ACBs should, as a general rule, involve developers in surveillance activities. For example, an ONC-ACB could request that a developer provide technical assistance to help the ONC-ACB understand and analyze variations of the health IT not seen during the testing and certification process and other complexities which will help to inform an ONC-ACB's understanding of its surveillance results. ONC-ACBs could also permit developers to assist ONC-ACBs to analyze and determine the causes of issues. ONC-ACBs should, however, be very careful to ensure that any assistance provided by a developer does not compromise the ONC-ACB's independence or the requirements of its accreditation. ONC-ACBs shall not take directions from developers about the locations at which surveillance will be carried out, or the surveillance methodology or approach to be employed.

There may be certain circumstances in which it would be inappropriate for ONC-ACBs to involve a developer in the conduct of ONC-ACB surveillance. For example, it would be inappropriate for an ONC-ABC to insist on the involvement of a developer if the ONC-ACB is conducting reactive surveillance in response to a complaint made by a provider about the performance of its health IT, and that provider has indicated that it is concerned about the risk of reprisal from the developer.

Developer Participation

Surveillance plans should describe how the ONC-ACB will establish and implement processes and controls to, if necessary, avoid disclosing a complainant's identity (and/or, as relevant, the identity of a complainant's employer/facility/organization) when conducting reactive surveillance.

As we explained in the 2015 Edition final rule, a developer should not take any action to frustrate the ability of an ONC-ACB to carry out its surveillance responsibilities. Ready access to certified health IT that has been deployed in a production environment is essential to an ONC-ACB's ability to conduct in-the-field surveillance. Therefore, if a developer were to take reprisal measures against a health care provider on the basis of their participation in surveillance activities, the ONC-ACB may regard the developer's actions as a refusal to participate in surveillance under the ONC Health IT Certification Program and institute appropriate procedures, consistent with the ONC-ACB's accreditation to ISO 17065, to suspend or withdraw the developer's certification. Additionally, we expect ONC-ACBs to notify ONC immediately if they become aware of a developer taking retaliatory measures against any health care provider who participates in ONC-ACB surveillance.

2. Working with Providers

a. Minimizing burden and accommodating provider preferences

Health care providers should be put to no greater burden when cooperating with in-the-field surveillance than is necessary for an ONC-ACB to fulfil its surveillance responsibilities. Depending upon the size and resources of a provider, different aspects of an ONC-ACB's surveillance approach will place a greater or lesser burden on the provider. ONC-ACBs should ensure that in-the-field surveillance is not carried out in a manner that unreasonably disrupts the workflow or operations of a provider. This might require ONC-ACBs to accommodate providers' schedules and other circumstances so that surveillance is carried out at a time and in a manner least likely to cause unreasonable disruption. This also requires that ONC-ACBs give providers ample notice of surveillance activities.

Individual health care providers are likely to have different preferences for how in-the-field surveillance should be approached in connection with their practice or facility. We expect that health care providers will be presented with a choice of evaluation approaches and be able to choose one that is most convenient for their practice. A health care provider's preference for a particular form of observation should be accommodated whenever practicable.

Minimizing Provider Burden

Surveillance plans should describe how the ONC-ACB will minimize the burden caused to health care developers by ONC-ACB surveillance and how the ONC-ACB will identify and then, if appropriate, accommodate provider preferences for the method and manner of ONC-ABC surveillance.

b. Procedures when contacting providers

While providers are given an option to attest to having cooperated with ONC-ACB surveillance as part of the reporting requirements promulgated under the QPP final rule,[16] they are under no requirement to do so. This means that a provider may choose not to cooperate with ONC-ACB surveillance activities without any adverse consequence to their standing under their respective programs. Accordingly, ONC-ACBs should be careful not to suggest in communications with health care providers that the provider is compelled, in any way whatsoever, to participate in or cooperate with the ONC-ACB's surveillance activities. However, an ONC-ACB is required to carefully and accurately document its efforts to complete in-the-field surveillance for each product and at each location (80 FR 62716), which would include documenting all instances of a health care provider's refusal to cooperate with ONC-ACB surveillance, or instances of a provider's failure to cooperate in good faith. CMS can then use this information for its programs.

Provider Cooperation with Surveillance Activities

Surveillance plans should describe the ONC-ACB's processes for documenting a provider's refusal to cooperate with surveillance activities, or the conduct of a provider that frustrates ONC-ACB surveillance activities.

C. Transparency and Disclosure Requirements: Surveillance of Developers' Disclosures

Developers must make a comprehensive disclosure of all known material information regarding their certified health IT—including limitations and additional types of costs (45 CFR 170.523(k)(1)). To comply with the disclosure requirements, a developer must disclose in plain language—on its website and in all marketing materials, communications statements, and other assertions related to its certified health IT—a detailed description of all **known material information** concerning limitations and additional types of costs that a person may encounter or incur to implement or use certified health IT capabilities, whether to meet meaningful use objectives and measures or to achieve any other use within the scope of the health IT's certification. Such information is "material" (and its disclosure therefore required) if the failure to disclose it could substantially interfere with the ability of a user or prospective user to implement

[16] This optional attestation requirement applies to MIPS eligible clinicians, eligible clinicians part of an APM Entity, EPs, eligible hospitals, and CAHs' (as those provider types are defined in the QPP final rule). See Medicare Program; Merit-Based Incentive Payment System (MIPS) and Alternative Payment Model (APM) Incentive Under the Physician Fee Schedule, and Criteria for Physician-Focused Payment Models, 81 FR 77008 (Nov 4, 2016) ("QPP final rule").

or use certified health IT for any use within the scope of the health IT's certification. Certain kinds of limitations and additional types of costs will always be material and thus, if known, must be disclosed. These include but are not limited to:

- Additional types of costs or fees (whether fixed, recurring, transaction-based, or otherwise) imposed by a developer (or any third-party from whom the developer purchases, licenses, or obtains any technology, products, or services in connection with its certified health IT) to purchase, license, implement, maintain, upgrade, use, or otherwise enable and support the use of capabilities to which health IT is certified; or in connection with any data generated in the course of using any capability to which health IT is certified (45 CFR 170.523(k)(1)(iv)(A)).
- Limitations, whether by contract or otherwise, on the use of any capability to which technology is certified for any purpose within the scope of the technology's certification; or in connection with any data generated in the course of using any capability to which health IT is certified (45 CFR 170.523(k)(1)(iv)(B)).
- Limitations, including but not limited to technical or practical limitations of technology or its capabilities, that could prevent or impair the successful implementation, configuration, customization, maintenance, support, or use of any capabilities to which technology is certified; or that could prevent or limit the use, exchange, or portability of any data generated in the course of using any capability to which technology is certified (45 CFR 170.523(k)(1)(iv)(C)).

We note that developers are not required to disclose information of which they are not and could not reasonably be aware, nor to account for every conceivable type of cost or implementation hurdle that a customer may encounter. "Developers are required, however, to describe **with particularity** the nature, magnitude, and extent of the limitations or types of costs" 80 FR 62601, 62722 (emphasis in original). A developer's disclosure possesses the requisite particularity if it contains sufficient information and detail from which a reasonable person under the circumstances would, without special effort, be able to reasonably identify the specific limitations he may encounter and reasonably understand the potential costs he may incur in the course of implementing and using capabilities for any purpose within the scope of the health IT's certification (80 FR 62601, 62722).

These requirements are explained in more detail in the Disclosure of Material Information Resource and in the 2015 Edition final rule, which also contains a number of hypothetical scenarios and accompanying analysis that will assist ONC-ACBs in understanding these requirements and incorporating them in their surveillance plans. We refer ONC-ACBs in particular to the discussion of these requirements at 80 FR 62722–24.

Transparency and Disclosure Requirements

Surveillance plans should describe:

- the ONC-ACB's approach to administering the mandatory disclosure requirements (45 CFR 170.523(k)(1)); and
- how the ONC-ACB will ensure that the ONC-ACB will access and review all relevant marketing materials, communications statements, and other assertions related to a developer's certified health IT as part of reactive surveillance of a product's compliance with mandatory disclosure requirements (45 CFR 170.523(k)(1)).

D. ONC Prioritized Capabilities and Requirements

We have prioritized the following capabilities:

2014 Edition	2015 Edition
Interoperability and Information Exchange	
• 45 CFR 170.314(b)(1) Transitions of care – receive, display and incorporate transition of care/referral summaries. • 45 CFR 170.314(b)(2) Transitions of care – create and transmit transition of care/referral summaries. • 45 CFR 170.314(b)(7) Data portability. • 45 CFR 170.314(b)(8) Optional – transitions of care. • 45 CFR 170.314(e)(1) View, download, and transmit to 3rd party. • 45 CFR 170.314(h)(1) Optional – Transmit - Applicability Statement for Secure Health. • 45 CFR 170.314(h)(2) Optional – Transmit - Applicability Statement for Secure Health Transport and XDR/XDM for Direct Messaging.	• 45 CFR 170.315(b)(1) (i) Transitions of care. • 45 CFR 170.315(b)(6) Data export • 45 CFR 170.315(e)(1) View, download, and transmit to 3rd party. • 45 CFR 170.315(g)(6) Consolidated CDA creation performance. • 45 CFR 170.315(g)(7) Application access - patient selection. • 45 CFR 170.315(g)(8) Application access - data category request. • 45 CFR 170.315(g)(9) Application access - all data request. • 45 CFR 170.315(h)(1) Transport methods and other protocols – Direct Project. • 45 CFR 170.315(h)(2) Transport methods and other protocols – Direct, Edge Protocol, and XDR/XDM.
Safety-related	
• 45 CFR 170.314(a)(2) Drug-drug, drug-allergy interaction checks. • 45 CFR 170.314(a)(8) Clinical decision support. • 45 CFR 170.314(a)(16) Inpatient setting only—electronic medication administration record. • 45 CFR 170.314(b)(4) Clinical information reconciliation. • 45 CFR 170.314(b)(9) Optional – Clinical information reconciliation and incorporation.	• 45 CFR 170.315(a)(4) Drug-drug, drug-allergy interaction checks for CPOE. • 45 CFR 170.315(a)(9) Clinical decision support (CDS). • 45 CFR 170.315(b)(2) Clinical information reconciliation and incorporation
Security	
• 45 CFR 170.314(d)(2) Auditable Events and Tamper-Resistance. • 45 CFR 170.314(d)(7) End-User Device Encryption.	• 45 CFR 170.315(d)(2) Auditable Events and Tamper-Resistance. • 45 CFR 170.315(d)(7) End-User Device Encryption.
Population Management	
• 45 CFR 170.314(c)(2) Clinical quality measures – import and calculate.	• 45 CFR 170.315(c)(1) Clinical quality measures – record and export.

We expect ONC-ACBs to cumulatively and thoroughly address these capabilities. In addition to the above capabilities, we consider the following additional elements to be a priority for surveillance:

- The assessment of developers' disclosures required by 45 CFR 170.523(k)(1) and the evaluation of potential non-conformities resulting from the failure to disclose material information about limitations or additional types of costs associated with certified health IT.[17]
- The assessment of potential non-conformities resulting from implementation or business practices of a developer that could affect the performance of certified capabilities in the field.
- The adequacy of developers' user complaint processes, including customer complaint logs, consistent with ISO/IEC 17065 § 4.1.2.2(j).[18]
- Appropriate use of the ONC Certified Health IT Certification and Design Mark.

Prioritized Capabilities and Requirements

Surveillance plans should describe the ONC-ACB's approach to addressing prioritized capabilities and requirements as part of their surveillance activities.

V. CORRECTIVE ACTION

When an ONC-ACB determines that a Complete EHR or Health IT Module does not conform to the requirements of its certification, the ONC-ACB must notify the developer of its findings and require the developer to submit a proposed corrective action plan for the applicable certification criterion, certification criteria, or certification requirement (45 CFR 170.556(d)).

Corrective Action

Surveillance plans should describe the procedures the ONC-ACB will follow for:

- Notifying the developer of its findings and requiring the developer to submit a proposed corrective action plan for the applicable certification criterion, certification criteria, or certification requirement. 45 CFR 170.556(d)(1).
- Providing direction to the developer as to the required elements of the corrective action plan. 45 CFR 170.556(d)(2).
- Determining what elements the developer must address as part of its corrective action plan, including an appropriate timeframe for completing corrective action under the circumstances, and evaluating and determining whether to approve, require revisions to, or reject a proposed corrective action plan submitted by a developer. 45 CFR 170.556(d)(3)–(4).
- Ensuring that proposed and revised corrective action plans are timely submitted and completed, or, if such plans are not timely submitted or completed, taking appropriate action to suspend or terminate the health IT's certification. 45 CFR 170.556(d)(5)–(6) and 170.556(f).
- Submitting (no less frequently than weekly) corrective action information to ONC for inclusion on the Certified Health IT Product List (CHPL). 45 CFR 170.523(f)(1)(xxii) & (f)(2)(xi).

[17] See Part IV.C for additional discussion of this element and its inclusion in ONC-ACBs' surveillance plans.

[18] See Part VII for additional information on this priority surveillance element.

Corrective Action Plan

ONC-ACBs must ensure prior to approving any corrective action plan that it contains, at a minimum, the following elements (45 CFR 170.556(d)(3)):

- A description of the identified non-conformities or deficiencies;
- An assessment of how widespread or isolated the identified non-conformities or deficiencies may be across all of the developer's customers and users of the certified Complete EHR or certified Health IT Module;
- How the developer will address the identified non-conformities or deficiencies, both at the locations under which surveillance occurred and for all other potentially affected customers and users;
- How the developer will ensure that all affected and potentially affected customers and users are alerted to the identified non-conformities or deficiencies, including a detailed description of how the developer will assess the scope and impact of the problem, including identifying all potentially affected customers; how the developer will promptly ensure that all potentially affected customers are notified of the problem and plan for resolution; how and when the developer will resolve issues for individual affected customers; and how the developer will ensure that all issues are in fact resolved.
- The timeframe under which corrective action will be completed.
- A requirement that the developer attest to having completed all elements of the corrective action plan (discussed below).

ONC-ACBs may also require any additional elements specified by the National Coordinator or that the ONC-ACB deems appropriate, consistent with its accreditation.

Corrective Action – Suspension:

Surveillance plans should describe the approach taken by the ONC-ACB to administering and managing the suspension of a certified product's certification pursuant to 45 CFR 170.556(d)(5) and the ONC-ACB's accreditation to ISO/IEC 17065, including:

- The length of time that the ONC-ABC will permit a product to be suspended before taking steps to withdraw the product's certification.
- The factors that the ONC-ACB considers when making a determination to lift a suspension or to withdraw the certification of a suspended product.

Corrective Action – Completion

Surveillance plans should outline the ONC-ACB's approach to verifying that developers have completed all requirements of corrective action specified in the approved corrective action plan. At a minimum, ONC-ACBs must detail an approach under which they will require developers to attest that the developer has completed all required elements of the plan and through which the ONC-ACB will validate that attestation. In this connection, we expect ONC-ACBs to verify that developers have notified all affected and potentially affected customers and users.

VI. SUBMISSION AND REPORTING OF SURVEILLANCE AND CORRECTIVE ACTION INFORMATION

A. Submission of Surveillance Information to ONC

The surveillance of certified health IT products is central to ONC's Health IT Certification Program, providing vital accountability for certified products. The surveillance reporting that ONC receives from ONC-ACBs plays a central role in informing ONC's understanding of the functioning of the Program, the nature of the health IT market, and the manner in which certified health IT is performing in the field.

Additionally, surveillance reporting provides vital accountability for the certification process itself. ONC carefully evaluates the surveillance reporting submitted by ONC-ACBs in order to satisfy itself that ONC-ACBs are fulfilling their surveillance responsibilities. As such, it is critical that ONC-ACBs provide comprehensive and detailed responses to all Program reporting requirements.

1. Surveillance Narratives and Corroborating Documentation

ONC-ACBs must report surveillance results to the National Coordinator on a rolling basis—and no less frequently than quarterly—throughout each calendar year (45 CFR 170.523(i)(2) and 170.556(e)). When submitting surveillance results, ONC-ACBs must identify each instance of surveillance (both reactive and randomized) performed during each calendar year and accurately report the results of their surveillance to ONC. ONC-ACBs must include sufficient information in surveillance reporting to allow ONC to determine, from the face of the report, that the ONC-ACB has satisfied the requirements of the ONC-ACB's surveillance plan, its accreditation, and the Principles of Proper Conduct for ONC-ACBs (45 CFR 170.523).

For each instance of surveillance carried out in a reporting period, the ONC-ACB must report the results of its surveillance and submit a detailed narrative about the facts and circumstances on which surveillance results are based, together with corroborating documentation and evidence to support its determination, including:

- Name of the developer of the certified Complete EHR or Health IT Module that was surveilled;
- Product name, product version and CHPL product number of the certified Complete EHR or Health IT Module that was surveilled;
- Type of surveillance initiated in each case (i.e., reactive or randomized);
- Date surveillance was initiated;
- Date surveillance completed (if completed at the time of reporting);
- Certification criteria and/or ONC Health IT Certification Program requirements surveilled; and

- Outcome of surveillance, using the following outcome categories:
    - ↳ No non-conformity; or
    - ↳ Non-conformity substantiated:
        - □ Resolved through corrective action;
        - □ Unresolved;
        - □ Corrective action ongoing;
        - □ Certification suspended;
        - □ Certification terminated; or
        - □ Other (provide description).
- For ***reactive*** surveillance:
    - ↳ Method of surveillance used (In-the-field; Controlled / Test Environment; or other specified method); and
    - ↳ Grounds on which the ONC-ACB initiated reactive surveillance (i.e., the particular facts and circumstances from which a reasonable person would have had grounds to question the continued conformity of the Complete EHR or Health IT Module).
- For ***reactive*** and ***randomized*** surveillance:
    - ↳ If no suspected non-conformities identified, the steps that the ONC-ACB took to surveil the certified Complete EHR or certified Health IT Module, to analyze evidence, and to arrive at its conclusion that there were no non-conformities;
    - ↳ If suspected non-conformities identified, the nature of the non-conformity or non-conformities that were substantiated;
    - ↳ If suspected non-conformities identified, the substantial factors that, in the ONC-ACB's assessment, caused or contributed to the suspected non-conformity or non-conformities (e.g., implementation problem, user error, limitations on the use of capabilities in the field, a failure to disclose known material information, etc.);
    - ↳ The steps taken by the ONC-ACB to engage and work with the developer and end-users to analyze and determine the causes of any suspected non-conformities and related deficiencies;
    - ↳ If a suspected non-conformity resulted from additional types of costs that a user was required to pay in order to implement or use the Complete EHR or Health IT Module's certified capabilities, the basis on which the ONC-ACB evaluated that suspected non-conformity;
    - ↳ If a suspected non-conformity resulted from limitations that a user encountered in the course of implementing and using the Complete EHR or Health IT Module's certified capabilities, the basis on which the ONC-ACB evaluated that suspected non-conformity;
    - ↳ If a suspected non-conformity resulted from the non-disclosure of material information by the developer about limitations or additional types of costs associated with the Complete EHR or Health IT Module, the basis on which the ONC-ACB evaluated the suspected non-conformity;
    - ↳ If an approved corrective action plan was received and completed, the steps taken by the ONC-ACB to verify that the developer had completed all requirements specified in the plan; and

↳ To assist ONC-ACBs to collate and submit their surveillance results to ONC, ONC has issued to ONC-ACBs a surveillance reporting template.

2. Reporting Surveillance Information on CHPL

Pursuant to the EOA final rule, ONC-ACBs are required to make all surveillance results publicly available on the Certified Health IT Product List (CHPL), including instances of surveillance where there are no discovered non-conformities (81 FR 72465). This new requirement increases the transparency and availability of information about certified health IT and provides customers and users of health IT with valuable information about the overall conformity of certified health IT to Program requirements. This requirement is in addition to the ONC-ACB requirement to submit surveillance reports to ONC.

In instances of surveillance where there are no determined non-conformities, the ONC-ACB should report on the CHPL all completed instances of these surveillance within 15 days of the end of each calendar year quarter. The ONC-ACB should not report ongoing surveillance in the CHPL where there are no determined non-conformities, until surveillance is completed. Where surveillance did determine a non-conformity, the ONC-ACB should report updates to the status of the surveillance weekly on the CHPL, as new information is available.

ONC-ACBs are required to report the following data elements on the CHPL for each and every surveillance episode (both reactive and randomized) (45 CFR 170.523(i)(2)):

- Name of the developer;
- Product name, product version;
- Type of surveillance initiated (i.e., reactive or randomized);
- Certification criteria and/or ONC Health IT Certification Program requirements surveilled;
- Date surveillance was initiated;
- Date surveillance completed;
- As applicable, the number of sites that were used in randomized surveillance; and
- Outcome of surveillance (i.e., Non-conformity or No Non-conformity).

In addition, ONC-ACBs are required to report the following data elements on the CHPL for each and every surveillance episode (both reactive and randomized) where a non-conformity was determined (45 CFR 170.523(f)(1)(xxii) & (f)(2)(xi)):

- The certification criteria that failed to confirm;
- A summary of the deficiency or deficiencies;
- The health IT developer's explanation of the deficiency or deficiencies (when available);
- The pass rate for each criterion in instances where the product was evaluated at more than one location (randomized surveillance only);
- The number of sites used in randomized surveillance;
- The date of the ONC-ACB's determination of the non-conformity;
- The date the ONC-ACB approved a corrective action plan;
- The date the corrective action began (may be before date of approval, but should be reflected in the corrective action plan);
- The date by which the corrective action must be completed;
- The data by which the corrective action was completed;

- A description of the resolution of the non-conformity or non-conformities.

Submission of Corrective Action Information

Surveillance plans should describe how ONC-ACBs will document and timely (no less frequently than weekly) submit each type of corrective action information to ONC for inclusion in the CHPL, as required by 45 CFR 170.523(f)(1)(xxii) & (f)(2)(xi).

B. Due Process and Exclusion of Certain Sensitive Information

1. Meaningful Opportunity for Input and Comment on ONC-ACB Findings

Consistent with its accreditation to ISO 17065 and with the Principles of Proper Conduct for ONC-ACBs, we expect an ONC-ACB to complete its review of all relevant facts and circumstances, including those raised by the developer in the course of the ONC-ACB's surveillance, prior to making a non-conformity or other determination and prior to submitting its surveillance results and, where applicable, corrective action information to the National Coordinator or making them publicly available via the CHPL (80 FR 62717–18 and 81 FR 72451).

Moreover, ONC-ACBs should provide developers with a meaningful opportunity to explain any deficiencies if the ONC-ACB makes a finding of non-conformity or potential non-conformity. When the developer has provided an explanation of the deficiencies identified by the ONC-ACB as the basis for its determination, the ONC-ACB must include the developer's explanation (subject to any exclusions described below) in its submission of this information to the National Coordinator (80 FR 62718).

2. Exclusion of Certain Information from Submission of Corrective Action Information and Surveillance Results

In submitting corrective action information and surveillance results to the National Coordinator, or in making surveillance results publicly available via the CHPL, ONC-ACBs must exclude any information that would identify any user or location that participated in or was subject to surveillance (80 FR 62725).

3. Exclusion of Certain Information from Submission of Corrective Action Information

With respect to the submission of corrective action information to the National Coordinator for inclusion in the CHPL, or the direct posting of corrective action information or surveillance results to the CHPL, ONC-ACBs should not submit any information that is in fact legally privileged or protected from disclosure and that therefore should not be listed on a publicly available website. ONC-ACBs may also implement other appropriate safeguards, as necessary, to protect information that, while not legally protected from disclosure, the ONC-ACB believes should not be reported to a publicly available website. We caution, however, that ONC-ACBs must ensure that such safeguards are narrowly tailored and consistent with the goal of promoting the greatest possible degree of transparency with respect to certified health IT and the business practices of certified developers, especially the disclosure of material information about limitations and types of costs associated with certified health IT. ONC-ACBs are required to accurately report the results of their surveillance and to explain in detail the facts and circumstances on which their conclusions are based.[19]

[19] Health IT developers are required to cooperate with these efforts and may not prevent or seek to discourage an ONC-ACB from reporting the results of its authorized surveillance activities. We note that while the ONC Health IT Certification Program is a voluntary one, developers who choose to participate agree to comply with certification Program requirements, including reporting requirements designed to ensure transparency and accountability for all participants and stakeholders (80 FR 62601, 62718).

C. Due Date and Submission Method for Surveillance Results

Surveillance results are due to ONC within 15 days of the end of each quarter, in the agreed upon template. ONC will only accept electronic submissions of surveillance result via ONC-ACB@hhs.gov.

ONC-ACBs are required to post identifiable surveillance results to the CHPL in the agreed upon template in accordance with the CHPL upload requirements.

VII. DEVELOPER COMPLAINT PROCESSES

A. Review of Developer Complaint Processes

ONC-ACBs are accredited to section 4.1.2.2(j) of ISO/IEC 17065, which instructs an ONC-ACB to ensure that a developer "keeps a record of all complaints made known to it relating to compliance with certification requirements and makes these records available to the certification body when requested." Section 4.1.2.2(j) also requires that the EHR technology developer "takes appropriate action with respect to such complaints and any deficiencies found in products that affect compliance with the requirements for certification," and "documents the actions taken."

Because developers are the primary recipients of complaints made about the performance of certified health IT, the proper handling by developers of complaints that raise Program conformity issues is central to the proper functioning of ONC's Health IT Certification Program. ONC-ACBs will evaluate the complaint processes of each developer whose technology was subject to surveillance during the applicable calendar year, and regardless of the circumstances that triggered surveillance or the type of surveillance performed.

We appreciate that because some developers provide helpdesk support for health IT users, it is possible that some developers will receive a high number of complaints, reports, and notifications about performance issues affecting their certified health IT. Some of these complaints, reports, or notifications will be complaints that raise questions about whether the certified health IT continues to comply with its certification requirements. Others will have no direct relevance to a certified health IT's certified capabilities. On this basis, it may not be feasible in some instances for an ONC-ACB to review all complaints and an ONC-ACB may elect to assess only a sample of the complaints log (or equivalent) maintained by a developer, so long as that sample is based on robust sampling and selection methodologies.

Accessing and Reviewing Developer Complaint Processes

Surveillance plans should describe:

- The ONC-ACB's processes for accessing and reviewing developers' complaint logs and any other information maintained by developers about complaints or issues reported to a developer;
- If the ONC-ACB does not propose to examine all complaints or issues reported to developers:
- a detailed justification for why it does not propose to review all complaints/issues and its rationale for why a sample is sufficient; and
- the sampling methodology used by the ONC-ACB to access and review a selection of complaints/issues;

- The frequency with which the ONC-ACB will access and review developers' complaint log and any other information maintained by a developer about complaints or issues reported to the developer;

Developer Compliance with Complaint Processes

Surveillance plans should describe how the ONC-ACB will identify, for each developer whose technology is subject to surveillance during the applicable calendar year, and regardless of the circumstances that triggered surveillance or the type of surveillance performed:

- The extent to which the developer followed the developer's complaint process, and any observed deficiencies with that process.
- The frequency of complaints made to the developer associated with the prioritized elements in Part IV.D above.

Responding to Developer Complaint Processes Information

Surveillance plans should describe how the ONC-ACB will determine when it will initiate reactive surveillance in response to becoming aware of a potential conformity issue as a result of the ONC-ACB's evaluation of the developer's complaint processes, including by identifying the factors that the ONC-ACB will consider and weigh when making its determination.

B. Reporting on Developer Complaint Processes

An ONC-ACB should report the results of its assessment of developer complaint processes, identifying for each developer whose technology was subject to surveillance during the applicable calendar year:

- The extent to which the developer followed its complaints process, and any observed deficiencies with its process.
- The frequency of complaints made to the developer associated with each of the prioritized elements in Part IV.D above (identified by reference to prioritized element).

VIII. PUBLIC ACCOUNTABILITY

ONC-ACBs are encouraged to publish their surveillance plans after submission to ONC. Making this information publicly available is consistent with our goal of making the Program more transparent and will improve the overall value stakeholders receive from the Program. ONC may at any time publish surveillance information to the extent permitted by law.